Q66458

Claims 1, 7, 11, 17, and 21
Cited literature: Japanese Unexamined Patent Application Publication 2000-235528

Remarks
Claims 1, 7, 11, 17, and 21
Cited Literature 1

Cited Literature 1 describes returning an electronically singed reception message (corresponding to the "certified response" of the present application) to the server relay unit (corresponding to the "first authentication means" of the present application) when the client relay unit (corresponding to the "second authentication means" of the present application) receives a message (corresponding to the "exchange message" of the present application), and also describes time-stamping the message. It is found that the client relay unit here stores messages from the server relay unit, as well as storing exchange messages between entities. Furthermore, since what volume of exchange messages is to be stored is something which can be suitably selected by a person skilled in the art, storing all exchange messages between entities is also something which could be easily thought of by a person skilled in the art. There cannot be said to be any remarkable technical difficulty in making the entity an electronic transaction entity or in stamping and storing messages.

拒絶理由通知書

特許出願の番号	特願２０００－２９８９３９
起案日	平成１７年　８月２６日
特許庁審査官	永野　志保　３３５０　５Ｓ００
特許出願人代理人	机　昌彦（外　２名）　様
適用条文	第２９条第２項

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記

請求項　１，７，１１，１７，２１
引用文献　特開２０００－２３５５２８号公報

備考
請求項　１，７，１１，１７，２１
引用文献　１
引用文献１には、クライアント中継部（本願の「第２の公証手段」に相当）が、メッセージ（本願の「交換メッセージ」に相当）を受信した際、サーバ中継部（本願の「第１の公証手段」に相当）に、電子署名を付加した受領メッセージ（本願の「証明応答」に相当）を返信することや、メッセージに時刻を打刻することも記載されており、クライアント中継部はサーバ中継部からのメッセージを記憶しており、エンティティ間の交換メッセージを記憶していると認められる。また、記憶する交換メッセージの量をどの程度にするかは当業者が適宜選択し得るものであるから、エンティティ間の全ての交換メッセージを記憶することも当業者が容易に思いつくことにすぎない。なお、エンティティを電子商取引エンティティとすることやメッセージに打刻して記憶することに格別な技術的困難性があるとはいえない。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

引 用 文 献 等 一 覧

補正では以下の点を注意されたい。

（1）明細書を補正した場合は、補正により記載を変更した個所に下線を引くこと。

（2）補正は、この出願の出願当初の明細書又は図面に記載した事項のほか、出願当初の明細書又は図面に記載した事項から自明な事項の範囲内で行わなければならない。補正の際には、意見書で、各補正事項について補正が適法なものである理由を、根拠となる出願当初の明細書等の記載箇所を明確に示したうえで主張されたい。

（3）なお、上記の補正等の示唆は法律的効果を生じさせるものではなく、拒絶理由を解消するための一案である。明細書等をどのように補正するかは出願人が決定すべきものである。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-235528
(43)Date of publication of application : 29.08.2000

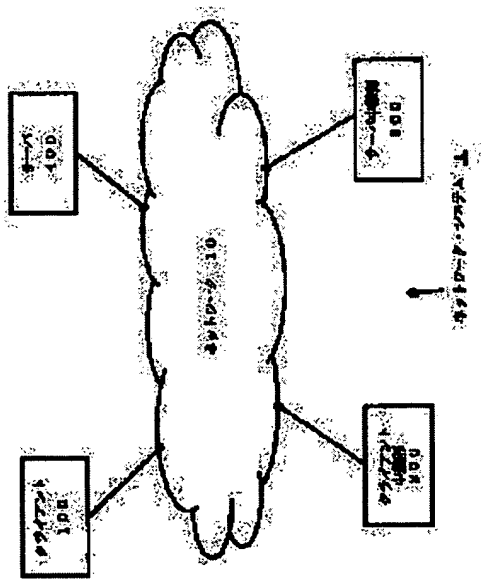
(51)Int.CI. G06F 13/00
G06F 9/46
G06F 15/00

(21)Application number : 11-038026
(22)Date of filing : 17.02.1999

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : HORIKIRI KAZUNORI

(54) METHOD FOR EXECUTING REMOTE PROCEDURE CALL ON NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain an excellent remote procedure call method capable of objectively certifying history information related to the execution of a remote procedure.
SOLUTION: Since a client repeating part 200 generates a 1st electronic signature corresponding to a request message and transmits the generated signature together with the request message, a server repeating part 300 can check the validity of the request message based on the 1st electronic signature. The server repeating part 300 generates a 2nd electronic signature corresponding to data synthesized from the request message and a response message and transmits the 2nd electronic signature together with the response message, so that the repeating part 200 can check the validity of the response message based on the 2nd signature. The repeating part 200 generates and transmits a 3rd electronic signature corresponding to data synthesized from the request message and the response message, so that the repeating part 300 can check the reception of the response message.



LEGAL STATUS

[Date of request for examination] 12.03.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－235528
（P2000－235528A）
(43)公開日　平成12年８月29日(2000.8.29)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｆ　５Ｂ０８５
9/46	３６０	9/46	３６０Ｂ　５Ｂ０８９
15/00	３３０	15/00	３３０Ａ　５Ｂ０９８

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－38026

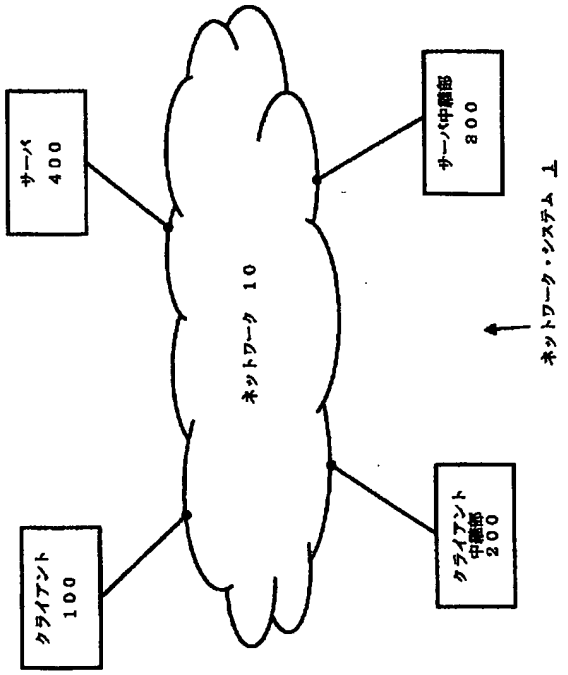
(22)出願日　平成11年２月17日(1999.2.17)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　堀切　和典
神奈川県足柄上郡中井町境430グリーンテクなかい　富士ゼロックス株式会社
(74)代理人　100086531
弁理士　澤田　俊夫

Ｆターム(参考)　5B085 AE00 BG07
5B089 GA11 GA21 HB04 HB05 JA00
JA11 JB03 KA13 MC03
5B098 AA10 GC16 JJ07

(54)【発明の名称】　ネットワーク上において遠隔手続き呼び出しを実行するための方法

(57)【要約】
【課題】　遠隔手続きの実行に関する履歴情報を客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供する。
【解決手段】　クライアント中継部は、要求メッセージに対する第１の電子署名を生成して要求メッセージとともに送信するので、サーバ中継部では、第１の電子署名を元に要求メッセージの正当性を検査することができる。サーバ中継部は、要求メッセージと応答メッセージを合成したデータに対する第２の電子署名を生成して応答メッセージとともに送信するので、クライアント中継部では、第２の電子署名を元に応答メッセージの正当性を検査することができる。クライアント中継部は、要求メッセージと応答メッセージを合成したデータに対する第３の電子署名を生成して送信するので、サーバ中継部では応答メッセージの受信を確認することができる。



1

【特許請求の範囲】

【請求項１】サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）クライアントが、遠隔手続き呼び出し方式の要求メッセージについての第１の電子署名を生成する段階と、（ｂ）クライアントが、要求メッセージを第１の電子署名とともに送信する段階と、（ｃ）サーバが、受信した要求メッセージに添付された第１の電子署名を検査する段階と、（ｄ）サーバが、要求メッセージに対する応答メッセージを生成する段階と、（ｅ）サーバが、要求メッセージと応答メッセージから合成されるデータに対して第２の電子署名を生成する段階と、（ｆ）サーバが、応答メッセージを第２の電子署名とともに送信する段階と、（ｇ）クライアントが、受信した応答メッセージの正当性を、第２の電子署名を元に検査する段階と、（ｈ）クライアントが、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第３の電子署名を生成する段階と、（ｉ）クライアントが、サーバに第３の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項２】（ｐ）サーバが、受信した要求メッセージと第１の電子署名を格納する段階、（ｑ）サーバが、第３の電子署名を格納する段階、（ｒ）クライアントが、第２の電子署名を格納する段階、のうち少なくとも１つを含むことを特徴とする請求項１に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項３】サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において、クライアント中継部とサーバ中継部の介在により遠隔手続き呼び出しを実行するための方法であって、（ａ）クライアントが、遠隔手続き呼び出し方式の要求メッセージをクライアント中継部に送信する段階と、（ｂ）クライアント中継部が、要求メッセージに対して第１の電子署名を生成する段階と、（ｃ）クライアント中継部が、サーバ中継部に対して、要求メッセージを第１の電子署名とともに送信する段階と、（ｄ）サーバ中継部が、第１の電子署名を元に受信した要求メッセージを検査する段階と、（ｅ）サーバ中継部が、サーバに要求メッセージを送信する段階と、（ｆ）サーバが、要求メッセージに対する応答メッセージを生成する段階と、（ｇ）サーバが、応答メッセージをサーバ中継部に送信する段階と、（ｈ）サーバ中継部が、要求メッセージと応答メッセージとから合成されるデータに対して第２の電子署名を生成する段階と、（ｊ）サーバ中継部が、応答メッセージを第２の電子署名とともに送信する段階と、（ｋ）クライアント中継部が、受信した応答メッセージの正当性を、第２の電子署名を元に検査する段階と、（ｌ）クライアント中継部が、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第３の電子署名を生成する段階と、（ｍ）クライアント中継部が、サーバ中継部に第３の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

2

【請求項４】（ｐ）サーバ中継部が、受信した要求メッセージと第１の電子署名を格納する段階、（ｑ）サーバ中継部が、第３の電子署名を格納する段階、（ｒ）クライアント中継部が、第２の電子署名を格納する段階、のうち少なくとも１つを含むことを特徴とする請求項３に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項５】遠隔手続き呼び出しを実行可能なネットワーク・システムであって、

遠隔手続き呼び出し方式の要求メッセージを生成するクライアントと、

要求メッセージに対する応答メッセージを生成するサーバと、

クライアントが要求メッセージを発行したこと及びクライアントがサーバからの応答メッセージを受理したことを客観的に証明するクライアント中継部と、

サーバが要求メッセージに対する応答メッセージを生成したことを客観的に証明するサーバ中継部と、を具備することを特徴とする遠隔手続きを実行可能なネットワーク・システム。

【請求項６】サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するクライアント中継部であって、

クライアントから要求メッセージを受信する手段と、

クライアントが生成した要求メッセージに対して第１の電子署名を生成する手段と、

第１の電子署名付きで要求メッセージを送信する手段と、

第２の電子署名付きで応答メッセージを受信する手段と、

第２の電子署名を元に受信した応答メッセージを検査する手段と、

要求メッセージと応答メッセージから合成されたデータに対して第３の電子署名を生成する手段と、

第３の電子署名を送信する手段と、

を含むことを特徴とするクライアント中継部。

【請求項７】さらに、第２の電子署名を記憶する手段を含むことを特徴とする請求項６に記載のクライアント中継部。

【請求項８】さらに、応答メッセージを記憶する手段を含むことを特徴とする請求項６に記載のクライアント中継部。

【請求項９】サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するサーバ中継部であって、
第１の電子署名付きで要求メッセージを受信する手段と、
第１の電子署名を元に要求メッセージを検査する手段と、
サーバに要求メッセージを送信する手段と、
サーバから応答メッセージを受信する手段と、
要求メッセージと応答メッセージから合成されたデータに対して第２の電子署名を生成する手段と、
第２の電子署名付きで応答メッセージを送信する手段と、
第３の電子署名を受信する手段と、を含むことを特徴とするサーバ中継部。

【請求項１０】さらに、要求メッセージと第１の電子署名、及び、第３の電子署名を記憶する手段を含むことを特徴とする請求項９に記載のサーバ中継部。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、１以上のサーバと１以上のクライアントからなる分散環境のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための遠隔手続き呼び出し方式に係り、特に、遠隔手続きの実行に関する履歴情報を客観的に証明するための遠隔手続き呼び出し方式に関する。

【０００２】更に詳しくは、本発明は、クライアントがサービス要求を行なったこと、サーバがサービス要求に対して応答したこと、クライアントがサーバからのサービス応答を受け取ったことを客観的に証明するための遠隔手続き呼び出し方式に関する。

【０００３】

【従来の技術】昨今の情報処理・情報通信の分野における発展は目覚しいものがある。この種の技術分野においては、コンピュータ・システム同士を相互接続するための研究・開発が、以前から活発になされてきた。システム同士を相互接続する主な目的は、複数ユーザによるコンピュータ資源の共有や、情報の共有・流通などである。

【０００４】システム間を接続するための伝送媒体すなわち「ネットワーク」としては、大学や事業所の構内など限られた空間内に敷設されたＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）の他、ＬＡＮを専用回線で接続したＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）や、一般公衆回線（ＰＳＴＮ）、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ）、インターネットなど様々である。

【０００５】ネットワーク・システムは、一般に、ネットワーク上の特定のコンピュータをサーバ（ファイル・サーバ，プリント・サーバ）とし、これを他のクライアントが利用し合うというクライアントーサーバ型として構築される。

【０００６】かかるクライアント・サーバ型モデルにおいては、クライアント側のプログラムを構成する一部の手続きの実行をネットワーク上の別のコンピュータに委託するというメカニズム、すなわち「遠隔手続き呼び出し（ＲＰＣ：ＲｅｍｏｔｅＰｒｏｃｅｄｕｒｅ Ｃａｌｌ）」、若しくは「遠隔メソッド呼び出し（ＲＭＩ：Ｒｅｍｏｔｅ Ｍｅｔｈｏｄ Ｉｎｖｏｃａｔｉｏｎ）」が用いられる。遠隔手続きの実行結果は、戻り値として、呼び出した側のコンピュータに返される。また、手許のコンピュータのキーボードやファイルを使ってプログラムへの入力を果たしたり、同じコンピュータのディスプレイやファイルに出力することもできる。

【０００７】遠隔手続き若しくは遠隔メソッド呼び出しの仕組みは、ＬＡＮの世界に限定されず、さらに、インターネットのような広域的なネットワーク上でも利用可能である。

【０００８】例えば、インターネット上には、ＷＷＷ（Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂ）と呼ばれる、ハイパーリンク構造の資源空間を提供する広域情報検索システムが公開されている。このＷＷＷ資源空間上では、ＨＴＴＰ（Ｈｙｐｅｒ ＴｅｘｔＴｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）の他，ＨＴＴＰＳ，Ｓ－ＨＴＴＰ（ｓｅｃｕｒｅ ＨＴＴＰ），ＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ），ＣＯＲＢＡ（Ｃｏｍｍｏｎ ＯＲＢ Ａｒｃｈｉｔｅｃｔｕｒｅ），ＩＩＯＰ（Ｉｎｔｅｒｎｅｔ Ｉｎｔｅｒ－ＯＲＢ Ｐｒｏｔｏｃｏｌ），ＪａｖａＲＭＩ（Ｒｅｍｏｔｅ Ｍｅｔｈｏｄ Ｉｎｖｏｃａｔｉｏｎ）などの各種プロトコルに従ってＷＷＷサーバとＷＷＷクライアント間でメッセージ交換が行なわれるが、これらは遠隔手続き／遠隔メソッド呼び出しの形態で実現される。このうちＨＴＴＰプロトコルについては、例えばＲＦＣ（Ｒｅｑｕｅｓｔ Ｆｏｒ Ｃｏｍｍｅｎｔｓ）１９４５やＲＦＣ２０６８に記述されている。

【０００９】ＷＷＷ上で特によく利用されるサービス資源は、ＨＴＭＬ（Ｈｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）という言語で記述された文書、すなわちハイパーテキストである。ＨＴＭＬについては、例えばＲＦＣ１８６６に記述されている。

【００１０】また、ＷＷＷサーバが所有する各資源は、ＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）という形式の識別子によって特定される。ＵＲＬとは、資源の名前とを指定した文字列であり、「スキーム名（プロトコル名）：／／ホスト名（ドメイン名）：ポート番号／パス名（ファイル名）」という形式で記述される。ＵＲＬについては、例えばＲＦＣ１７３

8やＲＦＣ１８０８などに記述されている。ここで言うホスト名は、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ネットワークで用いられるネーム・サービスであるＤＮＳ（ＤｏｍａｉｎＮａｍｅ Ｓｙｓｔｅｍ）の体系に従う。ＤＮＳでは、ドメインと呼ぶ論理的なグループを階層的に設定することができ、その論理グループの名称であるドメイン名をコンピュータの名前（ホスト名）の一部に組み込んで利用される。ＤＮＳサーバは、ドメイン名とＩＰアドレスの対応表を持っており、ドメイン名に基づく問い合わせに対して該当するＩＰアドレスを返すようになっている（周知）。

【００１１】ところで、旧来型のクライアント・サーバ・アプリケーションの構成では、クライアントとサーバが同一組織内のＬＡＮを経由して接続される方式が採用される。このような場合、クライアント側が呼び出した遠隔手続き呼び出しの実行処理は、通常、課金や計数の対象とはならない。これに対し、アプリケーションを構成するクライアントとサーバが異なる組織や団体で運営されているような場合、遠隔手続きを呼び出したクライアント（又はクライアントが属する組織）は、該手続きを実行したサーバ（又はサーバが属する組織）に対して、呼び出された手続きの実行に対する対価を支払う義務を負うと考えるのが相当であろう。特に、最近のネットワーク環境では、互いに異なる組織又は団体に帰属するクライアントとサーバとがインターネットのような外部ネットワークを介して接続されているので、後者のケースが非常に多くなってきている。

【００１２】ところが、呼び出された手続きの実行したという事実を、下記のように客観的に証明するような遠隔手続き呼出方式や装置は存在しない。

（１）クライアントがサービス要求したことを、後日客観的に証明できる。

（２）要求されたサービスに対してサーバが応答したことを、後日客観的に証明できる。

（３）サーバによるサービス応答をクライアントが受信したことを、後日客観的に証明できる。

【００１３】例えば、特開平１０－３１３３０８号公報には、ホームページ作成者の公開鍵証明書とホームページの固有情報への署名をサーバからクライアントにダウンロードして、クライアント側で署名検証処理を行う「ホームページ認証方法及び装置」について開示している。同公報によれば、１つのサーバに複数のホームページがあり、ホームページ毎に管理者が異なる場合であっても、サーバ単位ではなく、ホームページ単位でページ作成者の認証処理が可能となる。しかしながら、同公報によっても、クライアントがサーバに対して要求メッセージを送信したことや、クライアントがサーバからの応答メッセージを受信したことを、客観的に証明できる仕組みや機構については一切言及していない。

【００１４】また、特開平１０－１７１８８７号公報には、電子マネーを利用して取引する場合に、取引内容や決済が完了したことを客観的に証明できる電子データをオープンなネットワーク上で提供したオンラインショッピングシステムについて開示している。しかしながら、同公報に開示されたシステムでは、サーバがクライアントにサービスを提供する場合、クライアントが送信した要求メッセージをサーバが受信したことや、サーバが送信した応答メッセージをクライアントが受信したことなどを、客観的に証明するための仕組みや機構については全く言及していない。

【００１５】

【発明が解決しようとする課題】本発明の目的は、１以上のサーバと１以上のクライアントからなる分散環境のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求する、優れた遠隔手続き呼び出し方式を提供することにある。

【００１６】本発明の更なる目的は、遠隔手続きの実行に関する履歴情報を客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することにある。

【００１７】本発明の更なる目的は、クライアントがサービス要求を行なったこと、サーバがサービス要求に対して応答したこと、クライアントがサーバからのサービス応答を受け取ったことを客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することにある。

【００１８】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）クライアントが、遠隔手続き呼び出し方式の要求メッセージについての第１の電子署名を生成する段階と、（ｂ）クライアントが、要求メッセージを第１の電子署名とともに送信する段階と、（ｃ）サーバが、受信した要求メッセージに添付された第１の電子署名を検査する段階と、（ｄ）サーバが、要求メッセージに対する応答メッセージを生成する段階と、（ｅ）サーバが、要求メッセージと応答メッセージから合成されるデータに対して第２の電子署名を生成する段階と、（ｆ）サーバが、応答メッセージを第２の電子署名とともに送信する段階と、（ｇ）クライアントが、受信した応答メッセージの正当性を、第２の電子署名を元に検査する段階と、（ｈ）クライアントが、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第３の電子署名を生成する段階と、

（ｉ）クライアントが、サーバに第３の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【００１９】第１の側面に係るネットワーク上で遠隔手続き呼び出しを実行するための方法において、さらに、（ｐ）サーバが、受信した要求メッセージと第１の電子署名を格納する段階、（ｑ）サーバが、第３の電子署名を格納する段階、（ｒ）クライアントが、第２の電子署名を格納する段階、のうち少なくとも１つを含んでいてもよい。

【００２０】クライアントは、要求メッセージに対する第１の電子署名を生成し、且つ、第１の電子署名を添付して要求メッセージを送信するので、これを受け取ったサーバ側では、要求メッセージの正当性を検査したり確認することができる。また、サーバは、受信した要求メッセージと第１の電子署名を格納することによって、特定のクライアントから要求メッセージを受け取ったという事実を、後日客観的に証明することができる。

【００２１】また、サーバは、要求メッセージと応答メッセージを合成したデータに対する第２の電子署名を生成し、且つ、第２の電子署名を添付して応答メッセージを送信するので、これを受け取ったクライアント側では、応答メッセージの正当性を検査したり確認することができる。また、クライアントは、第２の電子署名を格納することによって、サーバから受け取った応答メッセージの内容を、後日客観的に証明することができる（例えば、不良な応答メッセージを戻されたという事実を証明することができる）。

【００２２】また、クライアントは、要求メッセージと応答メッセージを合成したデータに対する第３の電子署名を生成して送信するので、これを受け取ったサーバ側では、クライアントが応答メッセージを受け取ったことを確認することができる。また、サーバは、受信した第３の電子署名を格納することによって、クライアントに対して応答メッセージを送信したという事実を、後日客観的に証明することができる。

【００２３】また、本発明の第２の側面は、サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において、クライアント中継部とサーバ中継部の介在により遠隔手続き呼び出しを実行するための方法であって、（ａ）クライアントが、遠隔手続き呼び出し方式の要求メッセージをクライアント中継部に送信する段階と、（ｂ）クライアント中継部が、要求メッセージに対して第１の電子署名を生成する段階と、（ｃ）クライアント中継部が、サーバ中継部に対して、要求メッセージを第１の電子署名とともに送信する段階と、（ｄ）サーバ中継部が、第１の電子署名を元に受信した要求メッセージを検査する段階と、（ｅ）サーバ中継部が、サーバに要求メッセージを送信する段階と、（ｆ）サーバが、要求メッセージに対する応答メッセージを生成する段階と、（ｇ）サーバが、応答メッセージをサーバ中継部に送信する段階と、（ｈ）サーバ中継部が、要求メッセージと応答メッセージとから合成されるデータに対して第２の電子署名を生成する段階と、（ｊ）サーバ中継部が、応答メッセージを第２の電子署名とともに送信する段階と、（ｋ）クライアント中継部が、受信した応答メッセージの正当性を、第２の電子署名を元に検査する段階と、（ｌ）クライアント中継部が、少なくとも要求メッセージと応答メッセージから合成されたデータに対して第３の電子署名を生成する段階と、（ｍ）クライアント中継部が、サーバ中継部に第３の電子署名を送信する段階と、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【００２４】ここで、第２の側面に係るネットワーク上で遠隔手続き呼び出しを実行するための方法において、さらに、（ｐ）サーバ中継部が、受信した要求メッセージと第１の電子署名を格納する段階、（ｑ）サーバ中継部が、第３の電子署名を格納する段階、（ｒ）クライアント中継部が、第２の電子署名を格納する段階、のうち少なくとも１つを含んでいてもよい。

【００２５】クライアント中継部は、要求メッセージに対する第１の電子署名を生成し、且つ、第１の電子署名を添付して要求メッセージを送信するので、これを受け取ったサーバ中継部では、要求メッセージの正当性を検査したり確認することができる。また、サーバ中継部は、受信した要求メッセージと第１の電子署名を格納することによって、特定のクライアントからの要求メッセージを受け取ったという事実を、後日客観的に証明することができる。

【００２６】また、サーバ中継部は、要求メッセージと応答メッセージを合成したデータに対する第２の電子署名を生成し、且つ、第２の電子署名を添付して応答メッセージを送信するので、これを受け取ったクライアント中継部では、応答メッセージの正当性を検査したり確認することができる。また、クライアント中継部は、第２の電子署名を格納することによって、サーバが生成した応答メッセージの内容を、後日客観的に証明することができる（例えば、不良な応答メッセージを戻されたという事実を証明することができる）。

【００２７】また、クライアント中継部は、要求メッセージと応答メッセージを合成したデータに対する第３の電子署名を生成して送信するので、これを受け取ったサーバ中継部では、クライアント中継部（または、クライアント）が応答メッセージを受け取ったことを確認することができる。また、サーバ中継部は、受信した第３の電子署名を格納することによって、クライアントに対して応答メッセージを送信したという事実を、後日客観的に証明することができる。

【００２８】また、本発明の第３の側面は、遠隔手続きを実行可能なネットワーク・システムであって、遠隔手続き呼び出し方式の要求メッセージを生成するクライアントと、要求メッセージに対する応答メッセージを生成

するサーバと、クライアントが要求メッセージを発行したこと及びクライアントがサーバからの応答メッセージを受理したことを客観的に証明するクライアント中継部と、サーバが要求メッセージに対する応答メッセージを生成したことを客観的に証明するサーバ中継部と、を具備することを特徴とする遠隔手続きを実行可能なネットワーク・システムである。

【００２９】本発明の第３の側面に係るネットワーク・システムによれば、クライアントが要求メッセージを発行したことや、クライアントがサーバからの応答メッセージを受理したことなどの事実を、クライアント中継部が客観的に証明することができる。また、サーバが要求メッセージに対する応答メッセージを生成したことを、サーバ中継部が客観的に証明することができる。

【００３０】また、本発明の第４の側面は、サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するクライアント中継部であって、クライアントから要求メッセージを受信する手段と、クライアントが生成した要求メッセージに対して第１の電子署名を生成する手段と、第１の電子署名付きで要求メッセージを送信する手段と、第２の電子署名付きで応答メッセージを受信する手段と、第２の電子署名を元に受信した応答メッセージを検査する手段と、要求メッセージと応答メッセージから合成されたデータに対して第３の電子署名を生成する手段と、第３の電子署名を送信する手段と、を含むことを特徴とするクライアント中継部である。

【００３１】クライアント中継部は、さらに、第２の電子署名を記憶する手段や、応答メッセージを記憶する手段を含んでいてもよい。

【００３２】本発明の第４の側面に係るクライアント中継部は、要求メッセージに対する第１の電子署名を生成し、且つ、第１の電子署名を添付して要求メッセージを送信するので、これを受け取ったサーバ中継部やサーバでは、要求メッセージの正当性を検査したり確認することができる。また、サーバ中継部やサーバは、受信した要求メッセージと第１の電子署名を格納することによって、特定のクライアントからの要求メッセージを受け取ったという事実を、後日客観的に証明することができる。

【００３３】また、クライアント中継部は、要求メッセージと応答メッセージを合成したデータに対する第３の電子署名を生成して送信するので、これを受け取ったサーバ中継部やサーバでは、クライアント中継部（または、クライアント）が応答メッセージを受け取ったことを確認することができる。また、サーバ中継部やサーバは、受信した第３の電子署名を格納することによって、クライアントに対して応答メッセージを送信したという事実を、後日客観的に証明することができる。

【００３４】また、本発明の第５の側面は、サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において、クライアントとサーバ間の遠隔手続き呼び出し実行のために介在するサーバ中継部であって、第１の電子署名付きで要求メッセージを受信する手段と、第１の電子署名を元に要求メッセージを検査する手段と、サーバに要求メッセージを送信する手段と、サーバから応答メッセージを受信する手段と、要求メッセージと応答メッセージから合成されたデータに対して第２の電子署名を生成する手段と、第２の電子署名付きで応答メッセージを送信する手段と、第３の電子署名を受信する手段と、を含むことを特徴とするサーバ中継部である。

【００３５】サーバ中継部は、さらに、要求メッセージと第１の電子署名、及び、第３の電子署名を記憶する手段を含んでいてもよい。

【００３６】本発明の第５の側面に係るサーバ中継部は、要求メッセージと応答メッセージを合成したデータに対する第２の電子署名を生成し、且つ、第２の電子署名を添付して応答メッセージを送信するので、これを受け取ったクライアント中継部やクライアントでは、応答メッセージの正当性を検査したり確認することができる。また、クライアント中継部やクライアントは、第２の電子署名を格納することによって、サーバが生成した応答メッセージの内容を、後日客観的に証明することができる（例えば、不良な応答メッセージを戻されたという事実を証明することができる）。

【００３７】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３８】

【発明の実施の形態】以下、図面を参照しながら本発明の実施例を詳解する。

【００３９】図１には、本発明の実施に供されるネットワーク・システム１の構成を模式的に示している。ネットワーク・システム１は、データ（すなわちサービス要求メッセージやサービス応答メッセージなど）の伝送媒体であるネットワーク１０上に無数のデータ通信端末が接続されており、分散コンピューティング環境を提供している。以下、各部について説明する。

【００４０】ネットワーク１０は、例えば大学や企業の構内などの限られた空間内に敷設されたＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）である。あるいは、ＬＡＮ同士を専用線等で相互接続してなるＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）や、一般公衆回線（ＰＳＴＮ：Ｐｕｂｌｉｃ　Ｓｗｉｔｃｈｅｄ　Ｔｅｌｅｐｈｏｎｅ　Ｎｅｔｗｏｒｋ）、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ　Ｓｅｒｖｉｃｅ　Ｄｉｇｉｔａｌ　Ｎｅｔｗｏｒｋ）、これらネットワークの大規模な集合体で

あるインターネットであってもよい。各データ通信端末は、モデムやＴＡ（Ｔｅｒｍｉｎａｌ　Ａｄａｐｔｅｒ）、ＬＡＮアダプタ等を介してネットワーク１０に接続される。各データ通信端末同士は、ネットワーク１０を介して、例えばＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）接続されている。

【００４１】本実施例のネットワーク・システム１は、ネットワーク１０上の一部のデータ通信端末をサーバ４００とし、サーバ４００が提供するサービス資源を他の１以上のクライアント１００…が利用し合うという、分散環境のクライアントーサーバ型モデルとして構築されている。

【００４２】さらに、ネットワーク１０上には、クライアント中継部２００、及び、サーバ中継部３００が接続されている。これら中継部２００及び３００は、分散環境下でのクライアント１００及びサーバ４００間のメッセージ送受信において、電子署名を利用したメッセージの正当性の検査や確認を行ない、さらに送受信の記録をとり、後日客観的に証明したりする。各中継部２００及び３００の構成や処理動作については、後に詳解する。

【００４３】ネットワーク１０に接続された各データ通信端末は、サーバ或いはクライアントとしてデザインされた専用のマシンであってもよいが、多くの場合は、サーバ用、クライアント用、サーバ中継用、クライアント中継用の各アプリケーションを導入して動作する汎用のコンピュータ・システム（ワークステーションやパーソナル・コンピュータ等）である。

【００４４】サーバ４００は、複数のサービス資源を所有している。クライアント１００は要求メッセージを送信してサービス資源の提供を要求し、これに対して、サーバ４００は応答メッセージという形式でサービス資源を提供する。

【００４５】例えば、ネットワーク１０上に構築されたクライアントーサーバ型モデルがＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）であれば、ＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）プロトコルに従ってメッセージがネットワーク１０上を伝送する。この場合、サーバ４００が所有するサービス資源は、例えばホームページを形成するためのＨＴＭＬ（Ｈｙｐｅｒ　ＴｅｘｔＭａｒｋｕｐ　Ｌａｎｇｕａｇｅ）ファイルである。また、クライアント１００は、サーバのドメイン名を含んだＵＲＬ（Ｕｎｉｆｏｒｍ　ＲｅｓｏｕｒｃｅＬｏｃａｔｏｒ）の形式に従ってサービス資源を指定することができる（上述）。ＨＴＴＰに従ったサービス要求メッセージは、一種の遠隔手続き／メソッド呼び出しである。

【００４６】また、図２には、本発明の他の実施例に係るネットワーク・システム１の構成を模式的に示している。図１に係るネットワーク・システム１との相違は、クライアント中継部２００及びサーバ中継部３００の各々は、ネットワーク１０上で、独立したデータ通信端末としては存在せず、夫々、クライアント１００及びサーバ４００を構成する各コンピュータ・システム上で動作するクライアント中継用アプリケーション、サーバ中継用アプリケーションという形態で実装されている点である。図２に示す実施例の場合、クライアント１００とクライアント中継部２００の間、及びサーバ４００とサーバ中継部３００の間は、所定のプログラミング・インターフェースを介して接続されており、クライアント１００とクライアント中継部２００の間、及びサーバ４００とサーバ中継部３００の間がネットワーク接続されている図１に示す実施例とは相違する。

【００４７】クライアント中継部２００及びサーバ中継部３００の主業務は、分散環境下でのクライアント１００及びサーバ４００間のメッセージ送受信において、電子署名を利用したメッセージの正当性の検査や確認を行なうこと、さらに、送受信の記録をとり、後日客観的に証明することにある。図１及び図２のいずれの実施形態であっても、クライアント中継部２００及びサーバ中継部３００の各々において遂行される動作は本質的に同一である。以下の説明では、ネットワーク・システム１が図１又は図２のいずれであるかを区別しないこととする。

【００４８】なお、各中継部２００及び３００における電子署名方式として、例えば公開鍵暗号方式/*/を採用することができる。

【００４９】図３には、クライアント中継部２００の構成を模式的に示している。クライアント中継部２００は、要求署名生成部２１０と、記録部２２０と、送受信部２３０と、受領書生成部２４０と、応答メッセージ解析部２５０とで構成される。クライアント中継部２００の実体は、ネットワーク１０上の独立したデータ通信端末であっても、クライアント１００と同じコンピュータ・システム上で動作するクライアント中継用アプリケーションであってもよい。

【００５０】送受信部２３０は、ネットワーク１０経由でのメッセージ送受信を行なう。送受信部２３０が扱うメッセージは、例えば、クライアント１００から受け取る要求メッセージや、サーバ中継部３００から受け取る応答メッセージ、応答メッセージに対する受領メッセージ（後述）などである。

【００５１】記録部２２０は、要求署名生成部２１０、応答メッセージ解析部２５０、及び、受領書生成部２４０の各々からデータを受け取って、その保存を行なう。記録部２２０の実体は、例えば、クライアント中継部２００を構成するコンピュータ・システムにローカル接続されたハード・ディスク装置のような補助記憶装置である。

【００５２】要求署名生成部２１０は、クライアント１

００から受信した要求メッセージを要求先のサーバ４００に向けて転送するに際し、第１の電子署名ｓｉｇｎａｔｕｒｅ１を作成するための機能モジュールである。本実施例では、クライアント中継部２００は公開鍵暗号系の秘密鍵ｓｅｃｒｅｔｋｅｙ１を保持している。要求署名生成部２１０は、要求メッセージに対してこの秘密鍵ｓｅｃｒｅｔｋｅｙ１で電子署名を行なうようになっている。より具体的には、メッセージ中で要求されているパラメータに対して、要求番号と現在時刻と有効期限を表すビット列を連結して、秘密鍵ｓｅｃｒｅｔｋｅｙ１で電子署名して、要求メッセージとして送受信部２３０に出力する。

【００５３】応答メッセージ解析部２５０は、サーバ中継部３００から受信した応答メッセージを解析し検査するための機能モジュールである。本実施例では、応答メッセージ解析部２５０は、サーバ中継部３００の公開鍵ｐｕｂｌｉｃｋｅｙ２を保持しており、受信したメッセージを解析し、この公開鍵ｐｕｂｌｉｃｋｅｙ２を用いて応答メッセージ中の第２の電子署名ｓｉｇｎａｔｕｒｅ２を検証する。また、応答メッセージ解析部２５０は、この第２の電子署名ｓｉｇｎａｔｕｒｅ２を記録部２２０に転送して、これを保存する。

【００５４】なお、応答メッセージ解析部２５０は、サーバ中継部３００の公開鍵ｐｕｂｌｉｃｋｅｙ２の代わりに、ネットワーク１０で介在する認証局（図示しない）の公開鍵、又は、サーバ中継部３００の公開鍵と認証局の公開鍵の双方を用いてもよい。

【００５５】受領書作成部２４０は、サーバ中継部３００から応答メッセージを受信したことに応答して、その受領書を発行するための機能モジュールである。本実施例では、クライアント中継部１００は公開鍵暗号系の秘密鍵ｓｅｃｒｅｔｋｅｙ１を保持している。受領書作成部２３０は、応答メッセージ解析部２５０の出力に応じて、少なくとも要求メッセージ中のパラメータと応答メッセージから得られるメッセージ・ダイジェスト（後述）に対して秘密鍵ｓｅｃｒｅｔｋｅｙ１を用いて第３の電子署名ｓｉｇｎａｔｕｒｅ３を作成し、これを受領メッセージとして送受信部２３０に出力する。

【００５６】なお、クライアント中継部２００には、ＤＮＳサーバ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｅｒｖｉｃｅ：上述）によって、ホスト名”ｃｌｉｅｎｔ２００”が与えられているものとする。

【００５７】図４には、サーバ中継部３００の構成を模式的に示している。サーバ中継部３００は、応答署名生成部３１０と、記録部３２０と、送受信部３３０と、受領書解析部３４０と、要求メッセージ解析部２５０とで構成される。サーバ中継部３００の実体は、ネットワーク１０上の独立したデータ通信端末であっても、サーバ４００と同じコンピュータ・システム上で動作するサーバ中継用アプリケーションであってもよい。

【００５８】送受信部３３０は、ネットワーク１０経由でのメッセージ送受信を行なう。送受信部３３０が扱うメッセージは、例えば、クライアント中継部２００から受け取る要求メッセージや受領メッセージ、サーバ４００から受け取る応答メッセージなどである。

【００５９】記録部３２０は、応答署名生成部３１０、要求メッセージ解析部３５０、及び、受領書解析部３４０の各々からデータを受け取ってその保存を行なう。記録部３２０の実体は、例えば、サーバ中継部３００を構成するコンピュータ・システムにローカル接続されたハード・ディスク装置のような補助記憶装置である。

【００６０】応答署名生成部３１０は、サーバ４００から受信した応答メッセージを要求元のクライアント１００に向けて転送するに際し、第２の電子署名ｓｉｇｎａｔｕｒｅ２を作成するための機能モジュールである。本実施例では、公開鍵暗号系の秘密鍵ｓｅｃｒｅｔｋｅｙ２を保持している。応答署名生成部３１０は、応答メッセージに対してこの秘密鍵ｓｅｃｒｅｔｋｅｙ２で第２の電子署名を行ない、応答メッセージとして送受信部３３０に出力する。

【００６１】要求メッセージ解析部３５０は、クライアント中継部２００から受信した要求メッセージを解析し検査するための機能モジュールである。本実施例では、クライアント中継部２００の公開鍵ｐｕｂｌｉｃｋｅｙ１を保持している。要求メッセージ解析部３５０は、受信したメッセージを解析し、この公開鍵ｐｕｂｌｉｃｋｅｙ１を用いて要求メッセージ中の第１の電子署名ｓｉｇｎａｔｕｒｅ１を検証する。また、要求メッセージ解析部３５０は、この第１の電子署名ｓｉｇｎａｔｕｒｅ１を記録部３２０に転送して、これを保存する。

【００６２】受領書解析部３４０は、送受信部３３０を介して受け取った受領メッセージを解析するための機能モジュールであり、クライアント中継部２００の公開鍵ｐｕｂｌｉｃｋｅｙ１を用いて受領メッセージ中の第３の電子署名ｓｉｇｎａｔｕｒｅ３を検証する。また、要求メッセージ解析部３５０は、この第３の電子署名ｓｉｇｎａｔｕｒｅ３を記録部３２０に転送して、これを保存する。

【００６３】なお、サーバ中継部３００には、ＤＮＳサーバ（上述）によって、ホスト名”ｓｅｒｖｅｒ３００”が与えられているものとする。

【００６４】次に、クライアント中継部２００及びサーバ中継部３００を介して実現される、クライアント１００及びサーバ４００間のメッセージ送受信の動作手順について詳解する。

【００６５】以下では、ＨＴＴＰプロトコルを用いて、クライアント１００がクライアント中継部２００に第１の要求メッセージを送信し、クライアント中継部２００がサーバ中継部３００に第２の要求メッセージを送信し、サーバ中継部３００がサーバ４００に第３の要求メ

ッセージを送信する場合を例にとって説明する。但し、通信プロトコルはＨＴＴＰのみに限定されず、クライアント１００、クライアント中継部２００、サーバ中継部３００、及び、サーバ４００の各々は、ＨＴＴＰＳ，Ｓ－ＨＴＴＰ，ＦＴＰ，ＣＯＲＢＡ，ＩＩＯＰ，Ｊａｖａ ＲＭＩ，ＴＣＰ，ＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）などの任意の通信プロトコルを使用してもよい。

【００６６】まず、クライアント１００は、［数１］に示すような第１の要求メッセージを生成し、クライアント中継部２００に送信する。

【００６７】

【数１】

GET /service?a=1 HTTP/1.1

【００６８】クライアント中継部２００では、送受信部２３０が第１の要求メッセージを受信すると、これを要求署名生成部２１０に出力する。

【００６９】要求署名生成部２１０は、この第１の要求メッセージの中から要求パラメータとして”ａ＝１”を抽出する。

【００７０】次いで、要求署名生成部２１０は、メッセージ中に記されたサービス要求先”ｓｅｒｖｉｃｅ１”に該当するＵＲＬを、ＵＲＬ対応表の中で検索する。ＵＲＬ対応表は、例えば記録部２２０が保管しており（図示しない）、該当するＵＲＬは”ｈｔｔｐ：／／ｓｅｒｖｅｒ３００／ｏｂｊｅｃｔ３１０”であるとする。このＵＲＬは、要求したサービス資源がホスト名”ｓｅｒｖｅｒ３００”であるサーバが所有するオブジェクト名”ｏｂｊｅｃｔ３１０”という資源であることを示している。

【００７１】要求署名生成部２１０は、（シリアル番号，発行日時，有効期限，要求パラメータ）からなる第１の４項組を生成する。この場合の４項組は［数２］の通りとなる。

【００７２】

【数２】

(1, 199901081010, 199901081015, http://server300/object310?a=1)

【００７３】［数２］で示した４項組は、シリアル番号が１、要求の発行日時が世界時で１９９９年１月８日１０時１０分、要求の有効期限が１９９９年１月８日１０時１５分、要求パラメータが”ｈｔｔｐ：／／ｓｅｒｖｅｒ３００／ｏｂｊｅｃｔ３１０｜？ａ＝１”であることを示している。

【００７４】要求署名生成部２１０は、さらに、この第１の４項組に対してメッセージ・ダイジェスト関数を適用し、クライアント中継部２００が持つ公開鍵暗号系の秘密鍵ｓｅｃｒｅｔｋｅｙ１を用いて、第１の電子署名を生成する。この第１の電子署名を、”ｓｉｇｎａｔｕｒｅ１”とする。

【００７５】次いで、要求署名生成部２１０は、要求パラメータと第１の４項組と署名”ｓｉｇｎａｔｕｒｅ１”を送受信部２３０に出力する。

【００７６】送受信部２３０は、第１の４項組と要求パラメータを元に、［数３］に示すような第２の要求メッセージを、ネットワーク１０上に送信する。

【００７７】

【数３】

GET /object310?a=1 HTTP/1.1

Capability: (1, 199901081010, 199901081015, http://server300/object310?a=1)

Signature: signature1

【００７８】他方、サーバ中継部３００側の送受信部３３０は、第２の要求メッセージをネットワーク１０経由で受信すると、これを要求メッセージ解析部３５０に出力する。

【００７９】要求メッセージ解析部３５０は、以下の処理手順に従って、第２の要求メッセージを処理する。すなわち、

【００８０】（１）第２の要求メッセージを記録部３２０に送信する。記録部３２０は、これを保管し、クライアント１００から要求を受け取った事実を後日客観的に証明可能とする。

【００８１】（２）メッセージの先頭からサービス・オブジェクトの名前を抽出し、サーバ４００の第１のリファレンスを取得する。

【００８２】（３）ＨＴＴＰにおけるリクエスト・ヘッダの形式のうち、”Ｃａｐａｂｉｌｉｔｙ”というフィールド名に対応する値を抽出し、第１のケイパビリティとする。

【００８３】（４）ＨＴＴＰにおけるリクエスト・ヘッダの形式のうち、”Ｓｉｇｎａｔｕｒｅ”というフィールド名に対応する値を抽出し、第１の電子署名ｓｉｇｎａｔｕｒｅ１とする。

【００８４】（５）第１のケイパビリティの有効期限内か否かを検査する。期限内であれば、次ステップ（６）に進む。他方、期限が消滅していれば、当該ケイパビリティが無効である旨のメッセージを送受信部３３０に出力し、クライアント１００に向けて送信する。

【００８５】（６）第１のケイパビリティが無効ケイパビリティ集合に既に登録されているか否かを検査する。無効ケイパビリティ集合の中になければ、次ステップ（７）に進む。他方、当該ケイパビリティが無効ケイパビリティであれば、その旨のメッセージを送受信部３３０に出力し、クライアント１００に向けて送信する。

【００８６】（７）要求メッセージ解析部３５０は、第

１の電子署名ｓｉｇｎａｔｕｒｅ１が第１のケイパビリティの正しい署名であるか否かを検査する。該検査は、要求メッセージ解析部３５０が保持しているクライアント中継部２００の公開鍵ｐｕｂｌｉｃｋｅｙ１を用いて行なう。検査の結果、正しい署名であることが判明すれば、第１のケイパビリティを無効ケイパビリティ集合に追加して、要求の処理を続行する。他方、正しくない署名であれば、要求の処理を中止する。

【００８７】なお、ケイパビリティとは、要求元が要求するオブジェクトに対するアクセス権限等を記述した情報のことである。ケイパビリティの詳細については、例えば本出願人に既に譲渡されている特願平１０－２６６１４１号明細書を参照されたい。また、上述のステップ（６）及び（７）において、無効ケイパビリティ集合を用いるのは、同じケイパビリティが不正に再利用されるのを防止するためである。

【００８８】要求メッセージは、次いで、サーバ４００に送信される。これに対し、サーバ４００は、図５に示すような文書１を作成したとする。図示の通り、応答文書１は例えばＨＴＭＬ形式のコードである。

【００８９】サーバ中継部３００は、文書１で構成される第１の応答メッセージをサーバ４００から受け取ると、これを応答署名生成部３１０に渡す。

【００９０】応答署名生成部３１０では、少なくとも要求メッセージに含まれる要求パラメータ（この例では”ａ＝１”）と文書１とを連結した結果のメッセージ・ダイジェストに対して、サーバ中継部３００が持つ秘密鍵ｓｅｃｒｅｔｋｅｙ２で暗号化を行ない、第２の電子署名”ｓｉｇｎａｔｕｒｅ２”を生成する。そして、第２の電子署名ｓｉｇｎａｔｕｒｅ２を含んだ第２の応答メッセージを送受信部３３０に出力する。送受信部３３０は、これをクライアント中継部２００に送信する。

【００９１】また、応答署名生成部３１０は、要求パラメータと文書１とタイム・スタンプを連結した結果のメッセージ・ダイジェストに対して暗号化を行なうことで、第２の応答メッセージを生成するようにしてもよい。

【００９２】また、文字列を連結した後にメッセージ・ダイジェストを計算する処理を、以下のような連結を含まないメッセージ・ダイジェストの計算で置き換えてもよい。

【００９３】１：メッセージ・ダイジェストを初期化する。

２：要求パラメータを用いてメッセージ・ダイジェストを更新する。

３：文書１を用いてメッセージ・ダイジェストを更新する。

４：タイム・スタンプを用いてメッセージ・ダイジェストを更新する。

５：メッセージ・ダイジェストの終了処理を行う。

【００９４】クライアント中継部２００の送受信部２３０は、第２の応答メッセージを受信すると、これを応答メッセージ解析部２５０に出力する。

【００９５】応答メッセージ解析部２５０は、第２の応答メッセージとこれに添付された第２の電子署名”ｓｉｇｎａｔｕｒｅ２”とを検証する。また、クライアント中継部２００では、第２の電子署名”ｓｉｇｎａｔｕｒｅ２”と第２の応答メッセージを記録部２００に保存し、サーバ４００からいかなる応答メッセージが戻されたかを後日客観的に証明できるようにする。

【００９６】検証結果が正しい場合は、少なくとも要求メッセージと応答メッセージと現在時刻とを連結した結果のメッセージ・ダイジェストに対して秘密鍵ｓｅｃｒｅｃｔｋｅｙ１を用いて第３の電子署名”ｓｉｇｎａｔｕｒｅ３”を生成する。あるいは、要求メッセージと応答メッセージと現在時刻の各々のメッセージ・ダイジェストを連結した結果のメッセージ・ダイジェストに対して秘密鍵ｓｅｃｒｅｃｔｋｅｙ１で第３の電子署名”ｓｉｇｎａｔｕｒｅ３”を生成するようにしてもよい。そして、第３の電子署名”ｓｉｇｎａｔｕｒｅ３”を含んだ受領メッセージをサーバ中継部３００に送信する。

【００９７】サーバ中継部３００では、受信した受領メッセージを受領書解析部３４０に入力して解析及び検証する。

【００９８】受領メッセージが正しい場合は、記録部３２０にこれを保存し、クライアント中継部２００が応答メッセージを受領した事実を後日客観的に証明できるようにする。

【００９９】他方、受領メッセージが正しくない場合は、受領拒否メッセージをクライアント中継部２００に送信する。

【０１００】《注釈》＊：公開鍵暗号方式は、一方の鍵で暗号化すると他方の鍵でしか復号化できないという性質を持つ２個の暗号鍵で構成される。通常、暗号鍵の所有者は一方の鍵を第三者に流布する「公開鍵」として用い、他方の鍵を所有者自身が秘密管理する「秘密鍵」として用いる。送信者は、受信者の公開鍵でデータを暗号化することにより、受信者しか解読できない暗号メールの状態で安全にデータ送信することができる。また、公開鍵暗号方式の他の用途は、所謂「デジタル署名」である。公開鍵の所有者は自身の秘密鍵でデータを暗号化する。暗号データの受信者は、送信者の公開鍵を以って暗号データを復元できることから、送信者本人からの受信データであることを認証することができる。

【０１０１】［追補］以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。

【０１０２】例えば、上述した［発明の実施の形態］では、ＨＴＴＰプロトコルを利用した実施例を中心に説明

したが、本発明の要旨はＨＴＴＰプロトコルに限定されない。各データ通信端末（クライアント、クライアント中継部、サーバ中継部、サーバ）どうしが、ＨＴＴＰＳ，Ｓ－Ｈｔｔｐ，ＦＴＰ，ＣＯＲＢＡ，ＩＩＯＰ，ＪａｖａＲＭＩ，ＴＣＰ，ＵＤＰ等、他の任意の通信プロトコルを用いてメッセージ送受信する場合であっても、本発明を好適に適用することができることは言うまでもない。

【０１０３】要するに、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１０４】

【発明の効果】以上詳記したように、本発明によれば、遠隔手続きの実行に関する履歴情報を客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することができる。

【０１０５】また、本発明によれば、クライアントがサービス要求を行なったこと、サーバがサービス要求に対して応答したこと、クライアントがサーバからのサービス応答を受け取ったことを客観的に証明することができる、優れた遠隔手続き呼び出し方式を提供することができる。

【図面の簡単な説明】

【図１】　本発明の実施に供されるネットワーク・システム１の構成を模式的に示した図である。

【図２】　本発明の他の実施例に係るネットワーク・システム１の構成を模式的に示した図である。

【図３】　クライアント中継部２００の構成を模式的に示した図である。

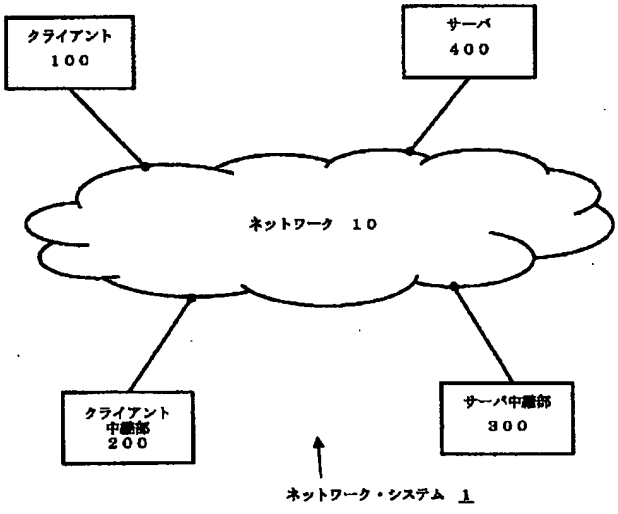
【図４】　サーバ中継部３００の構成を模式的に示した図である。

【図５】　サーバ４００が作成した応答メッセージの一例である。

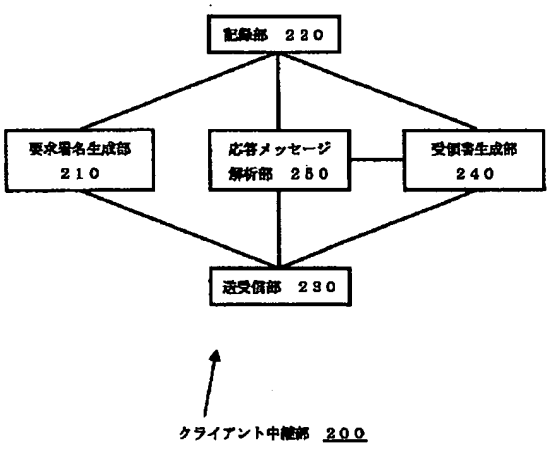
【符号の説明】

１…ネットワーク・システム、１０…ネットワーク、１００…クライアント、２００…クライアント中継部、２１０…要求署名生成部、２２０…記録部、２３０…送受信部、２４０…受領書生成部、２５０…応答メッセージ解析部、３００…サーバ中継部、３１０…応答署名生成部、３２０…記録部、３３０…送受信部、３４０…受領書解析部、３５０…要求メッセージ解析部、４００…サーバ。

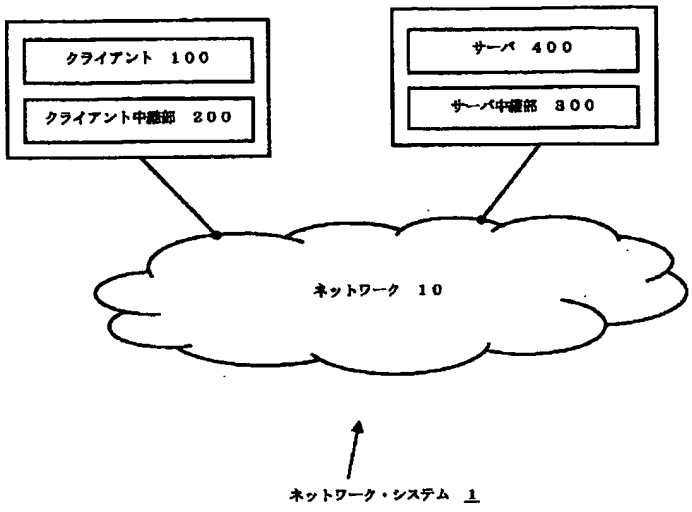
【図１】



【図３】



【図２】



【図５】

```
<tr>
<td>  aaaa100
<td>  100
<td>  1000
<tr>
<td>  aaaa200
<td>  200
<td>  2000
<tr>
<td>  aaaa300
<td>  300
<td>  3000
```

【図４】